Chapter 6

Finiteness for the number of equivalence classes

It is known that if $\mathcal{O}_S$ is the ring of S-integers in an algebraic number field K, then there are only finitely many $\mathrm{GL}(2, \mathcal{O}_S)$-equivalence classes of binary forms with coefficients in $\mathcal{O}_S$ of given degree and given discriminant. As it turns out, the analogous statement over function field is false. However we shall show that if $K = k(t)$ with k an algebraically closed fields of characteristic 0 and $\mathcal{O}_S$ is the ring of S-integers in K, then under certain conditions the binary forms with coefficients in $\mathcal{O}_S$ and of given degree and discriminant lie in finitely many $\mathrm{GL}(2, K)$-equivalence classes.

6.1 $\mathrm{GL}(2, K)$-equivalence classes

Let as usual k be a field with $k = \overline{k}, \mathrm{char}\, k = 0$ and $K = k(t)$, S a finite set of valuations containing ∞. Let $\alpha_1, \ldots, \alpha_s \in k$ be distinct and $p_i = t - \alpha_i, i = 1, \ldots, s$. Let $F \in \mathcal{O}_S[X, Y]$ and $\delta \in \mathcal{O}_S \backslash \{0\}$. Let L be a finite extension of K. For two binary forms $F_1, F_2 \in \mathcal{O}_S[X, Y]$ we say they are $\mathrm{GL}(2, K)$-equivalent if there exists $U \in \mathrm{GL}(2, K)$ and $\lambda \in K^*$ such that

$F_1 = \lambda(F_2)_U$, and they are $\mathrm{GL}\,(2, L)$-equivalent if the same holds when we replace K by L.

Fix $n \geqslant 4$, and consider the following two conditions:

$$\begin{cases} F \in \mathcal{O}_S[X, Y], D(F) \in \delta\mathcal{O}_S^{\times}, \\ F \text{ has splitting field } L \text{ over } K, \\ \deg F = n, \end{cases} \tag{6.1.1}$$

$$F \text{ is not } \mathrm{GL}\,(2, L)\text{-equivalent to a binary form in } k[X, Y]. \tag{6.1.2}$$

Theorem 6.1.1. *There are only finitely many* $\mathrm{GL}\,(2, K)$*-equivalence classes of binary forms satisfying (6.1.1) and (6.1.2).*

Proof. We reduce the $\mathrm{GL}\,(2, K)$-equivalence classes to $\mathrm{GL}\,(2, L)$-equivalence classes. We prove first that every $\mathrm{GL}\,(2, L)$-equivalence class of binary forms F with (6.1.1) is a union of finitely many $\mathrm{GL}\,(2, K)$-equivalence classes. Then it suffices to prove that there are only finitely many $\mathrm{GL}\,(2, L)$-equivalence classes of binary forms F with (6.1.1) and (6.1.2).

Fix a binary form F satisfying (6.1.1). It has a factorization

$$\begin{cases} F = a\prod_{i=1}^{n}(\alpha_i X + \beta_i Y), a \in K^* \\ (\sigma(\alpha_i), \sigma(\beta_i)) = (\alpha_{\sigma(i)}, \beta_{\sigma(i)}) \text{ for } i = 1, \ldots, n, \sigma \in \mathrm{Gal}(L/K), \end{cases} \tag{6.1.3}$$

where $(\sigma(1), \ldots, \sigma(n))$ is a permutation of $(1, \ldots, n)$ depending on F. For each $\sigma \in \mathrm{Gal}(L/K)$, there are only finitely many possibilities for the permutation of $(1, \ldots, n)$ associated with σ. So we may subdivide those $\mathrm{GL}\,(2, L)$-equivalence classes into subclasses under consideration such that two binary binary forms belong to the same subclass if and only if they satisfy (6.1.3) with the same permutation $(\sigma(1), \ldots, \sigma(n))$ for each $\sigma \in \mathrm{Gal}(L/K)$.

Now consider all binary forms in the same subclass. These are all $\mathrm{GL}\,(2, L)$-equivalent to one another and satisfy (6.1.3) with the same permutation $(\sigma(1), \ldots, \sigma(n))$. Fix one of such, $F_0 = a_0\prod_{i=1}^{n}(\alpha_{0i}X - \beta_{0i}Y)$. Let $F =$

$a\prod_{i=1}^{n}(\alpha_i X+\beta_i Y)$ be any other binary form in the same subclass. Then by definition there exists $V=\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\in \mathrm{PGL}\,(2,L)$ such that

$$V[\alpha_{0i}:\beta_{0i}]=[\alpha_{\tau(i)}:\beta_{\tau(i)}]\,(i=1,\dots,n), \tag{6.1.4}$$

with τ a permutation of $(1,\dots,n)$. We divide our subclass into finitely many smaller subclasses, such that two binary forms in the same smaller subclass satisfy (6.1.4) with the same permutation τ.

Let F_1, F_2 be two binary forms in the same smaller subclass, i.e., they are GL $(2, L)$-equivalent and satisfy (6.1.3) with the same permutations $(\sigma(1),\dots,\sigma(n))\,(\sigma\in \mathrm{Gal}(L/K))$ and (6.1.4) with the same τ. Assume

$$F_1=a_1\prod_{i=1}^{n}(\alpha_{1i}X+\beta_{1i}Y),$$
$$F_2=a_2\prod_{i=1}^{n}(\alpha_{2i}X+\beta_{2i}Y).$$

Then there exists $U\in \mathrm{PGL}\,(2,L)$ such that

$$U[\alpha_{1i}:\beta_{1i}]=[\alpha_{2i}:\beta_{2i}]\,(i=1,\dots,n), \tag{6.1.5}$$

because (6.1.4) holds true for the same τ. Without loss of generality, we assume that the U is represented by a matrix one of whose elements equals 1.

Applying each $\sigma\in \mathrm{Gal}(L/K)$ to (6.1.5), we obtain

$$\sigma(U)[\sigma(\alpha_{1i}):\sigma(\beta_{1i})]=[\sigma(\alpha_{2i}):\sigma(\beta_{2i})]\ (i=1,\dots,n,\sigma\in \mathrm{Gal}(L/K)).$$

By (6.1.3) and our subdivision we derive that

$$\sigma(U)[\alpha_{1\sigma(i)}:\beta_{1\sigma(i)}]=[\alpha_{2\sigma(i)}:\beta_{2\sigma(i)}]\,(\sigma\in \mathrm{Gal}(L/K),i=1,\dots,n).$$

Hence

$$\sigma(U)[\alpha_{1i}:\beta_{1i}]=[\alpha_{2i}:\beta_{2i}]\,(\sigma\in \mathrm{Gal}(L/K),i=1,\dots,n). \tag{6.1.6}$$

Now from (8.2.3) and (8.3.3) it follows that the images of $[\alpha_{1i} : \beta_{1i}]\,(i = 1, \ldots, n)$ under the projective transformation U and $\sigma(U)$ are equal. Since $n \geqslant 3$ and one of the entries of U is 1, this implies $\sigma(U) = U$ for any $\sigma \in \mathrm{Gal}(L/K)$. Hence $U \in \mathrm{PGL}\,(2, K)$. This means that F_1, F_2 are actually $\mathrm{GL}\,(2, K)$-equivalent, which proves the claim.

What remains is to prove that the binary forms with (6.1.1), (6.1.2) and (6.1.3) lie in only finitely many $\mathrm{GL}\,(2, L)$-equivalence classes.

Write $F = a\prod_{i=1}^{n}(\alpha_i X + \beta_i Y)$ with $a \in K^*$. Suppose $D(F) \in \delta\mathcal{O}_S^{\times}$. Let $R' = \mathcal{O}_S[\delta^{-1}]$. Then $D(F) \in R'^{\times}$. Let R'_L be the integral closure of R' in L. For $\theta_1, \ldots, \theta_r \in L$ we denote by $(\theta_1, \ldots, \theta_r)$ the fractional ideal with respect to R'_L generated by $\theta_1, \ldots, \theta_r$. Further, for a given polynomial P we denote by (P) the ideal of R'_L generated by the coefficients of P. Then by Gauss' Lemma we have

$$(F) = (a)\prod_{i=1}^{n}(\alpha_i, \beta_i). \tag{6.1.7}$$

Let $\Delta_{ij} = \alpha_i\beta_j - \alpha_j\beta_i$. Then

$$(\Delta_{ij}) \subseteq (\alpha_i, \beta_i)(\alpha_j, \beta_j) \text{ for } i, j = 1, \ldots, n, i \neq j. \tag{6.1.8}$$

Now we have

$$\begin{aligned}(1) \;&\supseteq\; \prod_{1\leqslant i<j\leqslant n}\Big(\frac{(\Delta_{ij})}{(\alpha_i, \beta_i)(\alpha_j, \beta_j)}\Big)^2\\ &=\; \frac{(a^{-2n+2}D(F))}{(a^{-2n+2})(F)^{2n-2}}\\ &=\; \frac{(D(F))}{(F)^{2n-2}}\\ &\supseteq\; (1),\end{aligned}$$

where the last equality is implied by the fact that $D(F) \in R'^{\times}$ and $F \in R'[X, Y]$. So we derive that (6.1.8) is actually an equality for every pair (i, j). Define the cross ratio

$$\rho_{ijhl}(F) := \frac{\Delta_{ij}\Delta_{hl}}{\Delta_{ih}\Delta_{jl}}.$$

Then $\rho_{ijhl}(F) \in R_L'^{\times}$ for all distinct $i, j, h, l \in \{1, \ldots, n\}$.

Lemma 6.1.2. *Let L be a finite extension of $k(t)$ and $\mathcal{O}_L$ the integral closure of $k[t]$ in L. The unit equation $x+y=1$ has only finitely many solutions x, y with $x, y \in \mathcal{O}_L \backslash k$ and all of them can be determined effectively in principle.*

Proof. See Theorem 1 and Theorem 2 of [17]. □

Lemma 6.1.3. *Suppose that $\frac{\Delta_{ij}\Delta_{hl}}{\Delta_{ih}\Delta_{jl}}$ lies in k^* for all tuples (i, j, h, l) in $\{1, \ldots, n\}$ with i, j, h, l distinct. Then F is* GL $(2, L)$*-equivalent to a binary form in $k[X, Y]$.*

Proof. Let $F = a\prod_{i=1}^{n}(\alpha_i X + \beta_i Y)$. Then there exists $U \in \mathrm{PGL}\,(2, L)$ such that

$$\begin{cases} U[\alpha_1 : \beta_1] = [1 : 0], \\ U[\alpha_2 : \beta_2] = [0 : 1], \\ U[\alpha_3 : \beta_3] = [1 : 1]. \end{cases} \tag{6.1.9}$$

So F is GL $(2, L)$-equivalent to a binary form of the shape

$$F' = a'XY(X+Y)\prod_{i=4}^{n}(\alpha_i' X + \beta_i' Y),$$

with $a' \in L^*$. Since the cross ratios remain invariant under a projective transformation, we have $\rho_{123i}(F') = 1 - \frac{\beta_i'}{\alpha_i'} \in k$ for $i \geqslant 4$. Hence $\frac{\beta_i'}{\alpha_i'} \in k$ and therefore $F' = bP$ with $b \in L^*, P \in k[X, Y]$. This proves the assertion. □

Now consider $F = a\prod_{i=1}^{n}(\alpha_i X + \beta_i Y), a \in K^*, n \geqslant 4$ with $D(F) \in R'^{\times}$. By (6.1.2) and Lemma 6.1.3, we may assume without loss of generality that $\rho_{1234} \notin k$. Since

$$\Delta_{12}\Delta_{34} + \Delta_{14}\Delta_{23} = \Delta_{13}\Delta_{24},$$

we have

$$\rho_{1234}(F) + \rho_{1432}(F) = 1.$$

But $\rho_{1234}(F), \rho_{1432}(F) \in R_L'^{\times}$, hence by Lemma 6.1.2, we know that there are only finitely many possibilities for $\rho_{1234}(F)$. For each choice $\lambda \in L \backslash k$

of $\rho_{1234}(F)$, consider all binary forms F with $\rho_{1234}(F) = \lambda$. There exists $U \in \mathrm{PGL}(2, L)$ such that (6.1.9) holds. So F is $\mathrm{GL}(2, L)$-equivalent to $XY(X+Y)\prod_{i=4}^{n}(\alpha_i' X + \beta_i' Y)$ with $\alpha_i' \neq 0$ for $i = 1, \ldots, n$. Since we have $\rho_{1234}(F) = 1 - \frac{\beta_4'}{\alpha_4'}$, we deduce that F is $\mathrm{GL}(2, L)$-equivalent to $XY(X+Y)(X+(\lambda+1)Y)$ if $n = 4$ or $XY(X+Y)(X+(\lambda+1)Y)\prod_{i=5}^{n}(X - \gamma_i Y)$ if $n \geqslant 5$. When $n > 4$, observe that for $i > 4$ we have $\rho_{123i}(F) = 1 + \gamma_i$ and $\rho_{124i}(F) = -1 - \frac{\lambda+1}{\gamma_i}$. These quantities cannot lie in k simultaneously since $\lambda \notin k$. Hence by applying Lemma 6.1.2 again, we infer that there are only finitely possibilities for $\gamma_i, i > 4$. It follows that there are only finitely many $\mathrm{GL}(2, L)$-equivalence classes of binary forms with (6.1.1), (6.1.2) and (6.1.3). This completes the proof.

□

Remark 6.1.4. The condition (6.1.2) cannot be relaxed to the condition that F not be $\mathrm{GL}(2, K)$-equivalent to a binary form in $k[X, Y]$. Here is a counter-example: fix $b \in K \backslash K^2$, consider all binary forms $F = X^4 + abX^2Y^2 + b^2Y^4, a \in k, a^2 \neq 4$. First, notice that the splitting field of such an F over K is $L = K(\sqrt{b})$, so F is $\mathrm{GL}(2, L)$-equivalent to $G = X^4 + aX^2Y^2 + Y^4 \in k[X, Y]$. However, F is not $\mathrm{GL}(2, K)$-equivalent to a binary form in $k[X, Y]$, since otherwise F would split into linear factors in K, contradicting the fact that $b \notin K^2$. Clearly, $F_a = X^4 + abX^2Y^2 + b^2Y^4$ and $F_{a'} = X^4 + a'bX^2Y^2 + b^2Y^4$ satisfy (6.1.1). Suppose F_a and $F_{a'}$ are $\mathrm{GL}(2, K)$-equivalent. Then $G_a = X^4 + aX^2Y^2 + Y^4$ and $G_{a'} = X^4 + a'X^2Y^2 + Y^4$ are $\mathrm{GL}(2, L)$-equivalent, hence being $\mathrm{GL}(2, k)$-equivalent. Let $c = \sqrt{a^2 - 4} \in k$. Then

$$G_a = (X - \lambda_1 Y)(X - \lambda_2 Y)(X - \lambda_3 Y)(X - \lambda_4 Y),$$

where $\lambda_1 = \sqrt{\frac{-a+c}{2}}, \lambda_2 = -\sqrt{\frac{-a+c}{2}}, \lambda_3 = \sqrt{\frac{-a-c}{2}}, \lambda_4 = -\sqrt{\frac{-a-c}{2}}$. The cross-ratio of $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ is

$$\lambda = \frac{(\lambda_1 - \lambda_2)(\lambda_4 - \lambda_3)}{(\lambda_1 - \lambda_3)(\lambda_4 - \lambda_2)} = \frac{4}{a+2}.$$

The cross ratios of the permutations of $(\lambda_1,\lambda_2,\lambda_3,\lambda_4)$ are

$$\begin{aligned} \lambda &= \frac{4}{a+2}, & \frac{1}{\lambda} &= \frac{a+2}{4}, \\ 1-\lambda &= \frac{a-2}{a+2}, & \frac{1}{1-\lambda} &= \frac{a+2}{a-2}, \\ \frac{\lambda}{\lambda-1} &= \frac{4}{2-a}, & \frac{\lambda-1}{\lambda} &= \frac{2-a}{4}. \end{aligned}$$

These are all one-to-one functions of a. Therefore, if $G_{a'}$ is $\mathrm{GL}(2,L)$-equivalent to G_a for some $a' \in k$, the corresponding cross-ratios remain the same, so there are at most six choices of a' such that $G_{a'}$ and G_a are $\mathrm{GL}(2,k)$-equivalent. This implies that when a runs through k, there are infinitely many $\mathrm{GL}(2,K)$-equivalence classes of binary forms of the form $F = X^4 + abX^2Y^2 + b^2Y^4$.

6.2 $\mathrm{GL}(2,\mathcal{O}_S)$-equivalence classes

Let $K = k(t)$ and S a finite set of valuations of K. We now show that a $\mathrm{GL}(2,K)$-equivalence class of binary forms with (6.1.1) is in general not a union of finitely many $\mathrm{GL}(2,\mathcal{O}_S)$-equivalence classes.

Lemma 6.2.1. *Let $F \in K[X,Y]$ with degree $\deg F \geqslant 3$ and $\mathrm{Aut}(F) := \{W \in \mathrm{PGL}(2,K) :$ there exists $\lambda \in K^*$ such that $F_W = \lambda F\}$. Then $\mathrm{Aut}(F)$ is finite.*

Proof. Let $W = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}(2,K), \lambda \in K^*$ such that $F_W = \lambda F$ and $F = \prod_{i=1}^{n}(\alpha_i X+\beta_i Y)$ with $\alpha_i,\beta_i \in \overline{K}$. Then $F_W = \prod_{i=1}^{n}\big((a\alpha_i+c\beta_i)X+(b\alpha_i+d\beta_i)Y\big)$. So there is a permutation σ of $(1,\dots,n)$ such that $[\sigma(\alpha_i):\sigma(\beta_i)] = [\alpha_i:\beta_i]W$ for $i = 1,\dots,n$. That is, W maps $n \geqslant 3$ distinct points in $\mathbb{P}^1(\overline{K})$ to n other distinct points. Hence W depends only on σ. Therefore $\#\mathrm{Aut}(F) \leqslant n!$. □

Let $U_1, U_2 \in \mathrm{GL}(2,K)$ with entries in $\mathcal{O}_S$. If F_{U_1} and F_{U_2} are $\mathrm{GL}(2,\mathcal{O}_S)$-equivalent, then by definition $F_{U_1} = \varepsilon F_{U_2 V}$ for some $V \in \mathrm{GL}(2,\mathcal{O}_S), \varepsilon \in k^*$.

Then $F_{(U_2V)^{-1}U_1} = \varepsilon F$ and so $(U_2V)^{-1}U_1 \in \mathrm{Aut}(F)$, hence $U_1 = U_2VW$ for some $W \in \mathrm{Aut}(F)$, in this case we say U_1 is *related* to U_2 *associated to* W and write $U_1 \equiv U_2\,(W)$.

Lemma 6.2.2. *Let $F \in K[X,Y]$ and $U \in \mathrm{GL}\,(2,K)$ with entries in $\mathcal{O}_S$ and $\det U = \delta$. Assume U_1, U_2 are related to U associated to the same $W \in \mathrm{Aut}(F)$ with $\det U_1, \det U_2 \in \delta\mathcal{O}_S^{\times}$. Then we have $U_1U_2^{-1} \in \mathrm{GL}\,(2,\mathcal{O}_S)$.*

Proof. By assumption we have

$$U_1^{-1}U = V_1(\lambda_1 W),\ U_2^{-1}U = V_2(\lambda_2 W),$$

for $V_1, V_2 \in \mathrm{GL}\,(2,\mathcal{O}_S)$ and $\lambda_1, \lambda_2 \in K^*$. Then $U_1^{-1}U_2 = \frac{\lambda_1}{\lambda_2}V_1V_2^{-1}$. But $\frac{\det U_1}{\det U_2} \in \mathcal{O}_S^{\times}$, hence $\frac{\lambda_1}{\lambda_2} \in \mathcal{O}_S^{\times}$. Therefore $U_1^{-1}U_2 \in GL(2,\mathcal{O}_S)$. This completes the proof. □

Theorem 6.2.3. *Let $F \in \mathcal{O}_S[X,Y]$ be a binary form of degree $n \geqslant 3$ and non-zero discriminant. Then there exists $D \in \mathcal{O}_S\backslash\{0\}$ with the following property: the binary forms $F' \in \mathcal{O}_S[X,Y]$ with*

$$\begin{cases} D(F') \in D\mathcal{O}_S^{\times}, \\ F' \text{ is } \mathrm{GL}\,(2,K)\text{-equivalence to } F \end{cases} \tag{6.2.1}$$

lie in infinitely many $\mathrm{GL}\,(2,\mathcal{O}_S)$-equivalence classes.

Proof. Suppose $S = \{\infty, p_1, \ldots, p_h\}$ and take $T = t$ if $S = \{\infty\}$ or $T = \prod_{i=1}^{h}(t-p_i)$ otherwise. Consider all binary forms F_U where $U \in \mathrm{GL}\,(2,K)$ has entries in $\mathcal{O}_S$ and $\det U = T^2 - 1$. Let $D = (T^2-1)^{n(n-1)}D(F)$. Suppose there are only finitely many $\mathrm{GL}\,(2,\mathcal{O}_S)$-equivalence classes of binary forms in $\mathcal{O}_S[X,Y]$ with the property (6.2.1). Then for every binary form F_V there exists U and $W \in \mathrm{Aut}(F)$ such that $V \equiv U\,(W)$.

Choose $U_1 = \left(\begin{smallmatrix} aT & 1 \\ 1 & bT \end{smallmatrix}\right)$, $U_2 = \left(\begin{smallmatrix} a'T & 1 \\ 1 & b'T \end{smallmatrix}\right)$ with $a, b, a', b' \in k$ satisfying $ab = a'b' = 1, a \neq a'$. Then U_1, U_2 have entries in $\mathcal{O}_S$ and $F_{U_1}, F_{U_2} \in \mathcal{O}_S[X,Y]$. But we have

$$U_1U_2^{-1} = \frac{1}{T^2-1}\begin{pmatrix} ab'T^2 - 1 & a'T - aT \\ b'T - bT & a'bT^2 - 1 \end{pmatrix}.$$

This is not in $\mathrm{GL}(2, \mathcal{O}_S)$ because for each $i = 1, \ldots, h$, $t - p_i$ is coprime with $T^2 - 1 = (T-1)(T+1)$.

Since k is algebraically closed, k is an infinite field, hence there are infinitely many matrices of the form U_1 and U_2. So there must be two matrices V, V' of form U_1, U_2 and $U \in \mathrm{GL}(2, K), W \in \mathrm{Aut}(F)$ such that $V \equiv U(W), V' \equiv U(W)$. This is a contradiction of the above and Lemma 6.2.2. □